PATENT

Attorney Docket No.: 020581-000700US

OPTIMIZED ENVELOPING VIA KEY REUSE

ABSTRACT OF THE DISCLOSURE

The present invention provides optimized enveloping for a public key cryptography system. A sender may reuse a secret key in multiple communications to a recipient without the need to recompute or re-encrypt the secret key. The first time a message is sent to a recipient, the sender generates and encrypts a secret key, then stores the secret key, the encrypted secret key, and associated counter data in a local data store. For subsequent messages to the recipient, the sender determines from the counter data whether the secret key may be reused; if the secret key is reused, the sender updates the counter data. A recipient stores previously received secret keys in a local data store in both encrypted and decrypted form. If an encrypted secret key in a received message matches an entry in the local data store, the recipient uses the previously decrypted secret key to decrypt the message.

SF 1294347 v1